Enhancing Security and Privacy in Local Area Network with TorVPN using Raspberry Pi As Access Point

Mohamad Afiqhakimi bin Rosli

Thesis submitted in fullfilment of the requirement for Bachelor of Science (Hons)
Data Communication and Networking
Faculty of Computer and Mathematical Sciences

December 2018

STUDENT DECLARATION

I certify that this thesis and the project to which it refers are the product of my own work and that any ideas or quotation from the work of other people, published or otherwise are fully acknowledged in accordance with the standard referring practices of the discipline.

……..
MOHAMAD AFIQHAKIMI BIN ROSLI
2016535173

DECEMBER 3, 2018

ABSTRACT

The Onion Router (Tor) service is one of the ways to surf out over the internet without being worried too much about the internet data theft and privacy of the information inside data packet. This service uses an Onion Routing technique to serve the encryption and anonymity for data packet that need to be send to the destination by bounce the data packet to several servers in another country which located inside the Tor relay. Inside Tor network, it needs at least three nodes in order to randomly bounce the data packet. These nodes were entry node, middle node, and exit node. Besides, to protect user's data packet inside local area network, one layer of encryption was needed. Virtual Private Network (VPN) was a suitable service which will ensure the encryption for data packets in local area network. Hence, the combination of Tor and VPN service was the best creation and method that needed for a normal user to enhance its security and privacy inside local area network while surfing over the Internet. The main objective of this project is to use Tor and VPN network over a public network by implementing the Tor and VPN service inside Raspberry Pi access point. Therefore, the clients connected to Raspberry Pi access point be able to use Tor and VPN service directly without any installation and configuration. There were two experiments involved in this project. The first is the confidentiality test which to verify its privacy in keeping the information securely. The second is the performance test of the internet connectivity in terms of ping, download and upload speed while Raspberry Pi access point used Tor and VPN service and shares its connection to the client to see how the internet connectivity performance would react when Tor service changed the access point's IP address. The results after the experiments were implemented was expected as the confidentiality tested on the Torvpn access point network showed the positive outcome by securing client's internet data packet travel through it. Going well also is the internet connectivity test while connected to VPN and Tor service, where the internet connectivity is not enough stable when the client's IP address changed to another IP address. Lastly, the used of combination VPN and Tor service inside local area network can be concluded that it is secure and suitable to use to secure the information as well as the data packet travel over the internet but does not suggest for user who wants a good internet connectivity.

TABLE OF CONTENTS